(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 400 362 A2**

(12) # EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **90108665.2**

(51) Int. Cl.5: **H04L 9/08**

(22) Anmeldetag: **08.05.90**

(30) Priorität: **31.05.89 DE 3917711**

(43) Veröffentlichungstag der Anmeldung:
05.12.90 Patentblatt 90/49

(84) Benannte Vertragsstaaten:
AT BE CH DE DK ES FR GB GR IT LI LU NL SE

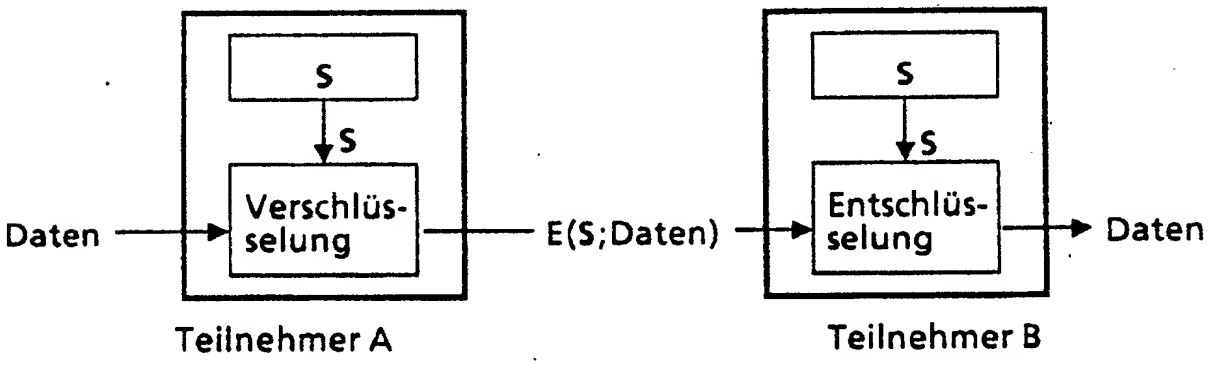
(71) Anmelder: **Siemens Aktiengesellschaft**
Wittelsbacherplatz 2
D-8000 München 2(DE)

(72) Erfinder: **Leclerc, Matthias, Dr.**
Theresienstrasse 140
D-8000 München 2(DE)

(54) **Verfahren zur hierarchischen Schlüsselverwaltung mit Teilschlüsseln zur Übermittlung digitalisierter Information.**

(57) Ein Verfahren zur hierarchischen Schlüsselverwaltung im Rahmen der Übermittlung digitalisierter Informationen über Kommunikationsnetze, wobei senderseitig und empfängerseitig jeweils informationsindividuell gleiche Schlüssel zum Ver- bzw. Entschlüsseln der betreffenden Informationen verwendet werden, bei dem vorgesehen ist, daß zumindest ein Sitzungsschlüssel, zumindest ein Terminalschlüssel und zumindest ein Austauschschlüssel verwendet werden, wobei der Sitzungsschlüssel der Verschlüsselung der während eines Übertragungsvorgangs gesendeten Information dient und von einer Zentrale erzeugt, an die beteiligten Terminals gesendet und nach Gebrauch gelöscht wird, daß der Sitzungsschlüssel zu seiner Übertragung jeweils unter den Terminalschlüsseln der Empfängerterminals verschlüsselt wird und daß eine Kommunikation zwischen zwei Zentralen durch den Austauschschlüssel verschlüsselt wird.

FIG 5



EP 0 400 362 A2

Verfahren zur hierarchischen Schlüsselverwaltung mit Teilschlüsseln zur Übermittlung digitalisierter Information

Die vorliegende Erfindung betrifft ein Verfahren zur hierarchischen Schlüsselverwaltung mit Teilschlüsseln zur Übermittlung digitalisierter Information sowie eine Schaltungsanordnung zur Durchführung des Verfahrens.

Die Übermittlung digitalisierter Informationen über Kommunikationsnetze erfordert oftmals die Gewährleistung der Geheimhaltung bzw. einen Beweis der Authentizität der Nachricht. Die hierzu verwendeten Mechanismen basieren im allgemeinen auf symmetrischen Verschlüsselungsverfahren, bei denen Sender und Empfänger mit demselben Schlüssel verschlüsseln und entschlüsseln. Aus Sicherheitsgründen sollte jede Nachricht mit einem eigenen Schlüssel versehen werden. Das wirft das Problem auf, Sender und Empfänger mit den entsprechenden Schlüsseln zu versorgen.

Bisher sind zwei verschiedene Verfahren bekanntgeworden, vgl. "W.F. Ehrsam, S.M. Matyas, C.H. Meyer und W.L. Tuchman: A cryptographic key management scheme for implementing the Data Encryption Standard", IBM-Systems 17, 106-125 (1978) und "M.E. Smid: Integrating the Data Encryption Standard into computer networks", IEEE Trans. Communications COMM-29, 762-722 (1981).

Der vorliegenden Erfindung liegt die Aufgabe zugrunde, ein Verfahren zu schaffen, das mehrere, verschiedene Schlüssel zur Sicherstellung der Geheimhaltung bzw. zum Beweis der Authentizität verwendet.

Zur Lösung dieser Aufgabe wird ein Verfahren gemäß dem Oberbegriff des Patentanspruchs 1 vorgeschlagen, das durch die in dem kennzeichnenden Teil angegebenen Merkmale charakterisiert ist.

Zur Realisierung des Verfahrens wird des weiteren erfindungsgemäß eine Schaltungsanordnung zur Durchführung dieses Verfahrens vorgeschlagen.

Im folgenden wird die vorliegende Erfindung anhand mehrerer Figuren im einzelnen beschrieben.

Fig. 1 zeigt in Form eines Blockschaltbildes einen sog. Sicherheitsmodul zur Durchführung des erfindungsgemäßen Verfahrens.

Fig. 2 zeigt ein Blockschaltbild entsprechend demjenigen gemäß Fig. 1, in das schematisch verschiedene Funktionsangaben S, S, T eingetragen sind.

Fig. 3 zeigt ein Blockschaltbild entsprechend demjenigen gemäß Fig. 1, in das schematisch die Funktion eines sog. Austauschschlüssels T^{ij} eingetragen ist.

Fig. 4 zeigt ein Blockschaltbild entsprechend demjenigen gemäß Fig. 1, das schematisch die Vorgänge bei einer sog. Umverschlüsselung eines Sitzungsschlüssels verdeutlicht.

Das erfindungsgemäße Verfahren unterscheidet zwischen sog. Sitzungsschlüsseln, sog. Terminalschlüsseln und sog. Austauschschlüsseln. Die Sitzungsschlüssel dienen der Verschlüsselung der während einer Verbindung gesendeten Information. Sie werden hierzu von einer Zentrale erzeugt, an die beteiligten Terminals gesendet und nach Gebrauch gelöscht.

Zur Übertragung der Sitzungsschlüssel von der Zentrale zu den Terminals werden die Sitzungsschlüssel unter den Terminalschlüsseln der Empfängerterminals verschlüsselt.

Die Kommunikation zwischen zwei Zentralen wird durch einen Austauschschlüssel verschlüsselt.

Die Terminals haben nur ihren eigenen Terminalschlüssel in einem zugriffssicheren Sicherheitsmodul abgespeichert. Die Zentrale hingegen muß alle Terminalschlüssel abspeichern. Dies erfordert einen hohen Speicherplatzbedarf: Bei beispielsweise 100 000 Terminals und Verschlüsselung mit der sog. DES-Technik ergibt sich (der log-Term bezieht sich auf die Adreßinformation): 100 000 x 56 Bit x $\log_2(100\,000)$ Bit = 7,3 MBit. Das System gemäß der vorliegenden Erfindung umgeht dieses Problem dadurch, daß die Terminalschlüssel on-line statt off-line erzeugt werden.

Zur Notation ist folgendes auszuführen:

Die Verschlüsselung einer Nachricht m unter dem Schlüssel S wird durch E(S;m) bezeichnet. Eine Einwegfunktion ist eine Abbildung, für die es rechentechnisch unmöglich ist, das Urbild eines Funktionswerts zu ermitteln.

Terminalschlüssel aus Teilschlüsseln

Jedem Terminal wird eine Identifikation $A \in [0...N-1]$ zugeordnet, die als

$A = a_0 + a_1 b + a_2 b^2 + ... + a_{k-1} b^{k-1}$

repräsentiert werden kann (für eine beliebige natürliche Zahl $b \geq 2$). Hierdurch wird ein Adreßvektor

$(a_0, a_1, a_2, ... a_{k-1})$

von Terminal A eindeutig bestimmt. Weiter sei

$$\begin{array}{llll} K_0(0), & K_0(1), & \ldots & , K_0(b-1) \\ K_1(0), & K_1(1), & \ldots & , K_1(b-1) \\ & \ldots\ldots & & \\ K_{k-1}(0), & K_{k-1}(1), & \ldots & , K_{k-1}(b-1) \end{array}$$

ein Feld von bxk (geheimen) Teilschlüsseln. Unter Benutzung der Adresse (a_0, a_1, a_2, ..., a_{k-1}) wird der Terminalschlüssel T des betreffenden Terminals durch

$T: = f(K_0(a_0) \oplus K_1(a_1) \oplus \ldots \oplus K_{k-1}(a_{k-1}))$

berechnet (f bezeichnet eine Einwegfunktion und "⊕" die bitweise Addition). Die Einwegfunktion verhindert, daß T durch Lösung von b x k linearen Gleichungen ermittelt werden kann.

Die einzelnen Terminalschlüssel werden bei den jeweiligen Terminals fest installiert. In der Zentrale muß nur das Teilschlüsselfeld gespeichert werden. Es bezeichne L die Länge eines Teilschlüssels. Die Speicherung des Feldes benötigt einen Speicherplatz von

$bxkxL = bx\log_b NxL \geq 3x\log_3 NxL$

Bits.

Schlüsselverwaltung

Das System baut auf drei im Sicherheitsmodul der Zentrale installierten Funktionen auf.

Sicherheitsmodul

Das Sicherheitsmodul ist ein physikalisch geschützter Bereich, in dem untergebracht sind:

- Register für Teil-, Sitzungs- und Austauschschlüssel,
- Ver- und Entschlüsselungseinheiten,
- ein Zufallsgenerator und
- die Hardware-Implementierung einer Einwegfunktion, vgl. Fig. 1.

Sowohl der Zufallsgenerator als auch die Einwegfunktion werden durch die Verschlüsselungsfunktion realisiert. Im ersten Fall wird zur Erzeugung einer Zufallszahl r die aktuelle Zeit t als Eingabe genommen und unter einem festen geheimen Schlüssel K verschlüsselt: r: = E(K;t). Eine Einwegfunktion f(x) wird durch Verschlüsselung einer Konstanten (etwa 0) unter dem als Schlüssel X interpretierten Argument x definiert:

f(x): = E(X;0).

Datenbusse führen als Ein- und Ausgabekanäle nach außen.

Umverschlüsselung eines Sitzungsschlüssels unter einem Terminalschlüssel

Im Zufallszahlengenerator wird ein Sitzungsschlüssel erzeugt, der im Register für Sitzungsschlüssel abgelegt wird.

Wie zuvor unter "Terminalschlüssel aus Teilschlüsseln" beschrieben, wird der Terminalschlüssel aus den jeweiligen Teilschlüsseln mit Hilfe der Einwegfunktion f berechnet. Durch die Angabe des Adreßvektors als Identifikation kann der Zugriff bes Mikroprogramms auf die einzelnen Teilschlüssel in effizienter Weise gesteuert werden.

In der Verschlüsselungseinheit wird E(T;S) berechnet, vgl. Fig. 2.

Umverschlüsselung eines Sitzungsschlüssels unter Austauschschlüssel

Der vertrauliche Datenfluß zwischen zwei Zentralen i und j wird durch Austauschschlüssel T^{ij} verschlüsselt. Diese Schlüssel sind wie Terminalschlüssel permanent installiert.

Als Beispiel sei angenommen, daß ein von der Zentrale i versorgtes Terminal mit einem von der Zentrale j versorgten Terminal kommunizieren will. Die Zentrale i erzeugt den erforderlichen Sitzungsschlüssel S und verschlüsselt ihn unter dem Austauschschlüssel T^{ij}, vgl. Fig. 3.

Umverschlüsselung eines Sitzungsschlüssels

Die Zentrale j erhält von der Zentrale i den verschlüsselten Sitzungsschlüssel $E(T^{ij};S)$. Zur Aussendung an das Empfängerterminal wird S unter dessen Terminalschlüssel umverschlüsselt. Hierzu wird zunächst $E-(T^{ij};S)$ entschlüsselt und S in das Register der Sitzungsschlüssel geladen. Der Terminalschlüssel T wird wie beschrieben erzeugt und S unter T verschlüsselt, vgl. Fig. 4.

Terminalverschlüsselung

Die Terminals besitzen ihre Terminalschlüssel nur in geschlossener Form. Sie sind nur in der Lage, die Ver- und Entschlüsselungsfunktion unter einem Sitzungsschlüssel oder ihrem Terminalschlüssel auszuführen.

Fig. 5 stellt exemplarisch die Kommunikationsverschlüsselung dar.

Ansprüche

1. Verfahren zur hierarchischen Schlüsselverwaltung im Rahmen der Übermittlung digitalisierter Informationen über Kommunikationsnetze, wobei senderseitig und empfängerseitig jeweils informationsindividuell gleiche Schlüssel zum Ver- bzw. Entschlüsseln der betreffenden Informationen verwendet werden,
dadurch gekennzeichnet,
- daß zumindest ein Sitzungsschlüssel, zumindest ein Terminalschlüssel und zumindest ein Austauschschlüssel verwendet werden, wobei der Sitzungsschlüssel der Verschlüsselung der während eines Übertragungsvorgangs gesendeten Information dient und von einer Zentrale erzeugt, an die beteiligten Terminals gesendet und nach Gebrauch gelöscht wird,
- daß der Sitzungsschlüssel zu seiner Übertragung jeweils unter den Terminalschlüsseln der Empfängerterminals verschlüsselt wird und
- daß eine Kommunikation zwischen zwei Zentralen durch den Austauschschlüssel verschlüsselt wird.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
daß die Terminals jeweils nur ihren eigenen Terminalschlüssel in einem sog. zugriffssicheren Sicherheitsmodul abgespeichert enthalten.

FIG 1

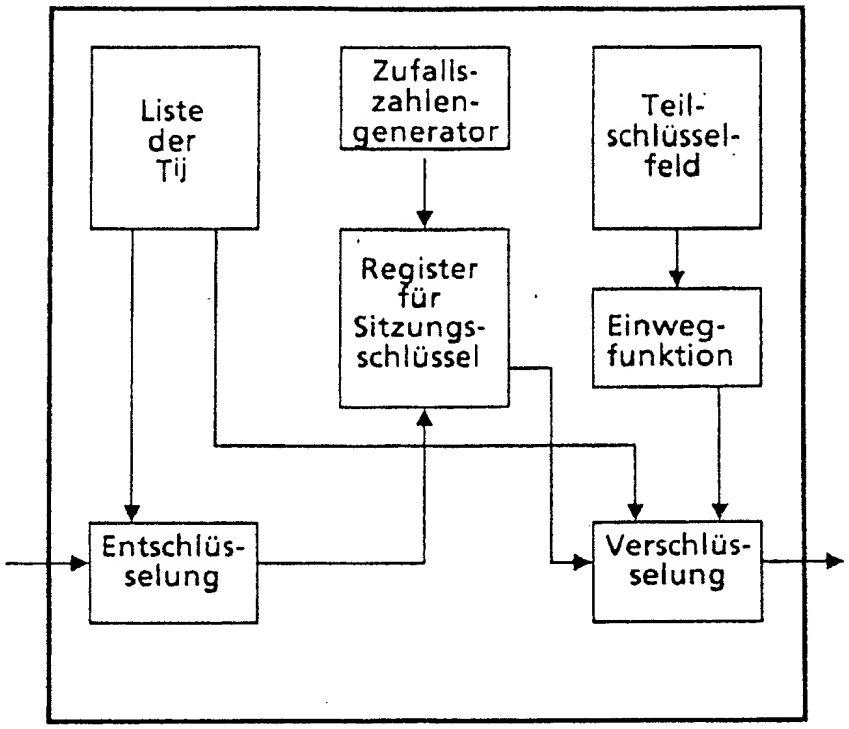

Liste der Tij
Zufalls-zahlen-generator
Teil-schlüssel-feld
Register für Sitzungs-schlüssel
Einweg-funktion
Entschlüs-selung
Verschlüs-selung

FIG 2

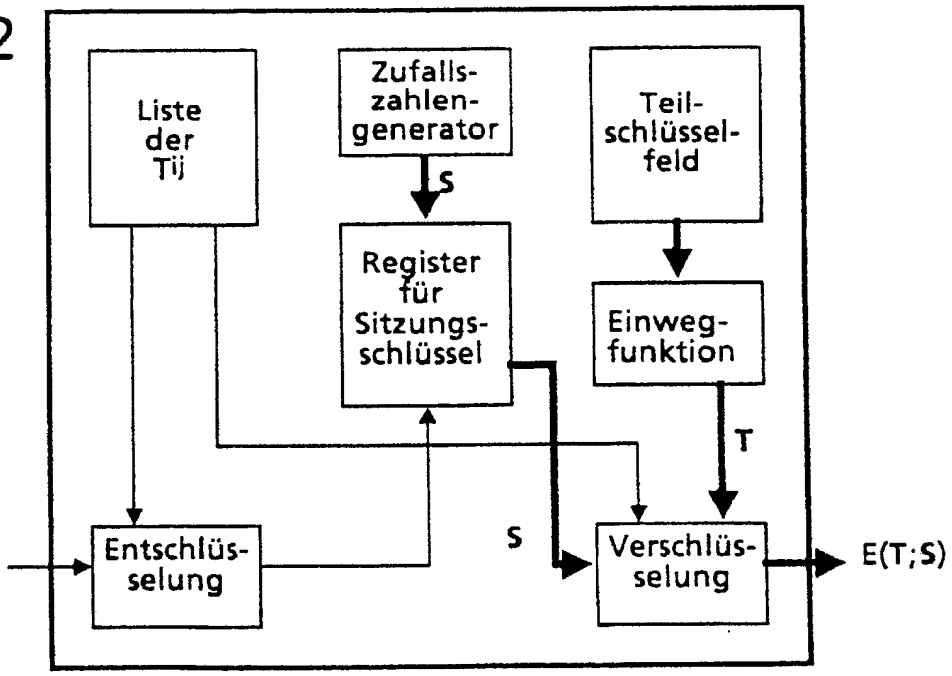

Liste der Tij
Zufalls-zahlen-generator
S
Teil-schlüssel-feld
Register für Sitzungs-schlüssel
Einweg-funktion
T
S
Entschlüs-selung
Verschlüs-selung
E(T;S)

FIG 3

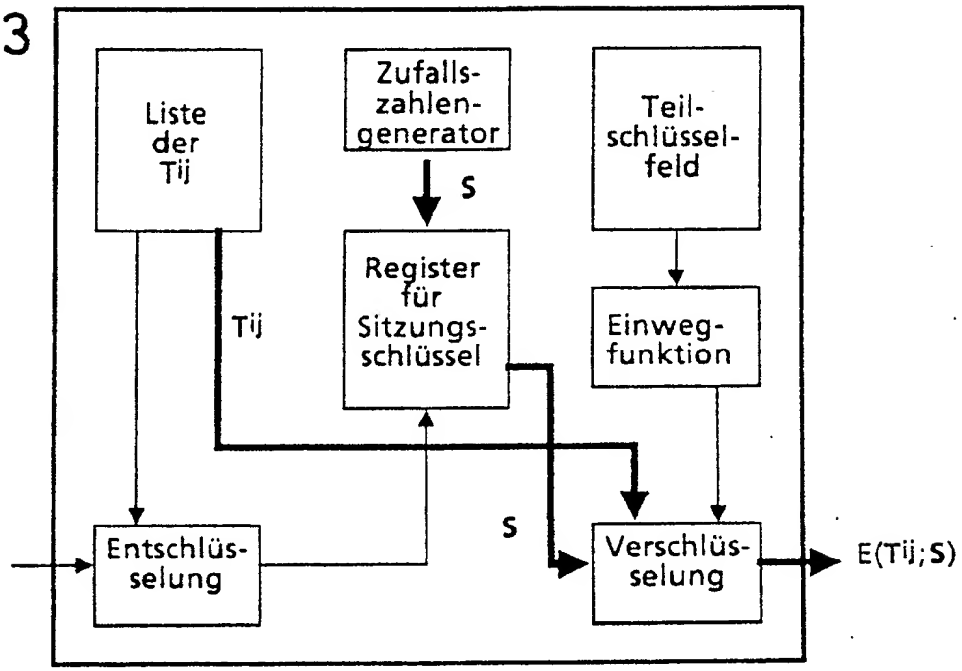

Liste der Tij
Zufalls-zahlen-generator
S
Teil-schlüssel-feld
Register für Sitzungs-schlüssel
Tij
Einweg-funktion
Entschlüs-selung
S
Verschlüs-selung
E(Tij;S)

FIG 4

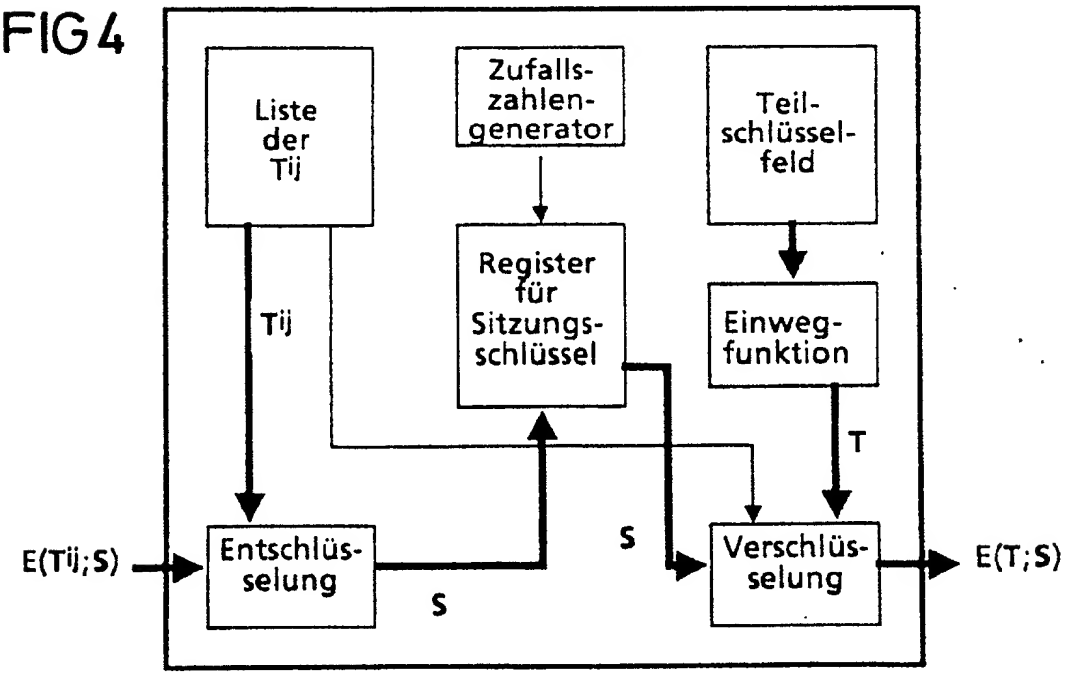
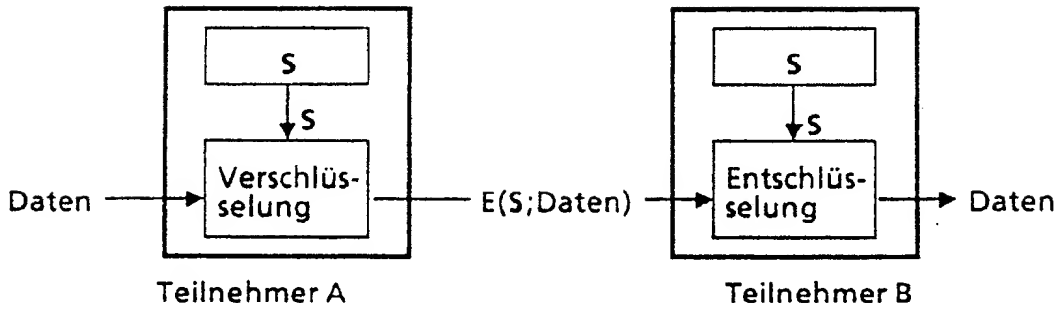

Liste der Tij
Zufalls-zahlen-generator
Teil-schlüssel-feld
Register für Sitzungs-schlüssel
Tij
Einweg-funktion
T
E(Tij;S)
Entschlüs-selung
S
S
Verschlüs-selung
E(T;S)

FIG 5


S
S
Verschlüs-
selung
Daten
E(S;Daten)
S
S
Entschlüs-
selung
Daten
Teilnehmer A
Teilnehmer B

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 400 362 A3**

(12) # EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **90108665.2**

(51) Int. Cl.5: **H04L 9/08**

(22) Anmeldetag: **08.05.90**

(30) Priorität: **31.05.89 DE 3917711**

(43) Veröffentlichungstag der Anmeldung:
05.12.90 Patentblatt 90/49

(84) Benannte Vertragsstaaten:
BE DE DK ES FR GB GR IT LU NL

(88) Veröffentlichungstag des später veröffentlichten Recherchenberichts: **27.05.92 Patentblatt 92/22**

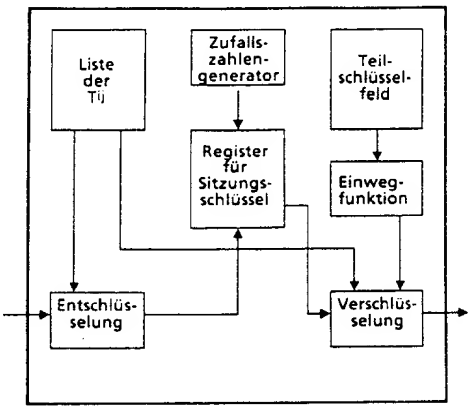
(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT**
Wittelsbacherplatz 2
W-8000 München 2(DE)

(72) Erfinder: **Leclerc, Matthias, Dr.**
Theresienstrasse 140
W-8000 München 2(DE)

(54) **Verfahren zur hierarchischen Schlüsselverwaltung mit Teilschlüsseln zur Übermittlung digitalisierter Information.**

(57) Ein Verfahren zur hierarchischen Schlüsselverwaltung im Rahmen der Übermittlung digitalisierter Informationen über Kommunikationsnetze, wobei senderseitig und empfängerseitig jeweils informationsindividuell gleiche Schlüssel zum Ver- bzw. Entschlüsseln der betreffenden Informationen verwendet werden, bei dem vorgesehen ist, daß zumindest ein Sitzungsschlüssel, zumindest ein Terminalschlüssel und zumindest ein Austauschschlüssel verwendet werden, wobei der Sitzungsschlüssel der Verschlüsselung der während eines Übertragungsvorgangs gesendeten Information dient und von einer Zentrale erzeugt, an die beteiligten Terminals gesendet und nach Gebrauch gelöscht wird, daß der Sitzungsschlüssel zu seiner Übertragung jeweils unter den Terminalschlüsseln der Empfängerterminals verschlüsselt wird und daß eine Kommunikation zwischen zwei Zentralen durch den Austauschschlüssel verschlüsselt wird.

FIG 1



EP 0 400 362 A3

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung

EP 90 10 8665

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int. Cl.5)
X	PROCEEDINGS OF THE 1986 IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 7-9 April 1986, pages 138-147, Washington DC, US; W.P.LU and M.K. SUNDARESHAN: "A Hierarchical Key Management Scheme For End-to-End Encryption In Internet Environments" * Seite 138, linke Spalte, Zeile 27 - Zeile 42 * * Seite 138, rechte Spalte, Zeile 11 - Zeile 26 * * Seite 140, linke Spalte, Zeile 8 - rechte Spalte, Zeile 7 * * Seite 140, rechte Spalte, letzter Absatz * * Abbildungen 2a, 2b *	1,2	H04L9/08
A	EP-A-0 281 224 (HEWLETT-PACKARD) * Seite 4, Zeile 3 - Zeile 11 * * Abbildung 1 *	2	

RECHERCHIERTE SACHGEBIETE (Int. Cl.5)

H04L

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	26 MAERZ 1992	LYDON Michael

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus andern Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P0403)